Robert B. Hawk (Bar No. 118054)
Clay James (Bar No. 287800)
Maren J. Clouse (Bar No. 228726)
HOGAN LOVELLS US LLP
4085 Campbell Avenue, Suite 100
Menlo Park, California 94025
Telephone: + 1 (650) 463-4000
Facsimile: + 1 (650) 463-4199
robert.hawk@hoganlovells.com
clay.james@hoganlovells.com
maren.clouse@hoganlovells.com

Attorneys for Defendant
APPLE INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-CV-00453-JST

DEFENDANT APPLE INC.'S NOTICE OF MOTION AND MOTION TO DISMISS SECOND CONSOLIDATED AMENDED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

The Honorable Jon S. Tigar

Date: December 2, 2014
Time: 2:00 p.m.
Courtroom: 9, 19th Floor

THIS DOCUMENT RELATES TO ALL ACTIONS:

Opperman v. Path, Inc., No. 13-cv-00453-JST
Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple, Inc., No. 12-cv-1529-JST
Gutierrez v. Instagram, Inc., No. 12-cv-6550-JST

NOTICE OF MOTION AND MOTION TO DISMISS SECOND CONSOLIDATED AMENDED COMPLAINT

TO ALL PARTIES AND THEIR COUNSEL OF RECORD: PLEASE TAKE NOTICE THAT on December 2, 2014 at 2:00 p.m., or as soon thereafter as the matter may be heard by the Court, in the Courtroom of the Honorable Jon Tigar, located at the Phillip Burton Federal Building & United States Courthouse, 450 Golden Gate Avenue, 19th Floor, San Francisco, California, Defendant Apple Inc., by and through its attorneys of record, will, and hereby does, move the Court for an order dismissing with prejudice the Second Consolidated Amended Complaint.

This motion will be made based on Federal Rules of Civil Procedure 8, 9(b), and 12(b)(6) and Article III of the U.S. Constitution. This motion also will be based upon this Notice; the attached Memorandum of Points and Authorities; the concurrently filed Request for Judicial Notice; the January 8, 2014 Request for Judicial Notice in Support of Defendant Apple Inc.'s Reply in Support of Motion to Dismiss (Dkt. No. 437); the October 12, 2012 Declaration of Mark Buckley in Support of Apple Inc.'s Motion to Dismiss (Dkt. No. 147-1); the complete files and records of this action; and such other matters and arguments as may come before the Court, including those raised in connection with reply briefing and oral argument relating to this motion.

Dated: August 22, 2014

HOGAN LOVELLS US LLP

By: */s/Robert B. Hawk*
Robert B. Hawk

Attorneys for Defendant
APPLE INC.

ISSUES PRESENTED

1. Do Plaintiffs' fraud-based claims (UCL, FAL, CLRA and Deceit) fail because Plaintiffs have not pled facts showing reliance on a specific identified misrepresentation, because Plaintiffs have not pled facts supporting an inference that the alleged misrepresentations were communicated to Plaintiffs through a long-term advertising campaign as described in the *Tobacco II* case, and because Plaintiffs fail to plead any actionable omission?
2. Do Plaintiffs' claims for conversion and intrusion upon seclusion against Apple, asserted based on allegations that Apple aided and abetted the alleged wrongdoing of the App Defendants, fail because Plaintiffs have failed to plead the requisite elements of aiding and abetting liability?
3. Does Plaintiffs' claim for Conversion independently fail because Plaintiffs have failed to plead facts showing injury—necessary to support Article III standing and the requisite element of damage?
4. Do Plaintiffs lack standing to assert a claim for injunctive relief?
5. Does the Communications Decency Act, 47 U.S.C. § 230, preclude each of Plaintiffs' claims to the extent they are based on anything other than a misrepresentation by Apple?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

Dismissing all 16 of Plaintiffs' claims against Apple in the prior Complaint, this Court provided a detailed roadmap regarding the nature and specificity of allegations that would be required if Plaintiffs were to successfully amend. The Court, for example, dismissed Plaintiffs' Conversion claim because Plaintiffs lacked "Article III standing based on any injury to their property rights in their address books." The Court further found that all of Plaintiffs' misrepresentation claims failed, because they did not allege reliance on any particular representation, and had not adequately alleged a long-term advertising campaign of the kind that would excuse them from pleading specific reliance. Yet now, in pleading their Second Consolidated Amended Complaint ("SAC")—pared down to six counts—Plaintiffs again come up short.

With respect to their "misrepresentation" counts (Counts 3-6), Plaintiffs once more fail to plead individual reliance or a long-term advertising campaign. No named Plaintiff alleges that he or she relied on, or even saw, any specific actionable statement by Apple. And, as for the alleged "long-term advertising campaign," Plaintiffs make out no campaign at all. Instead, Plaintiffs cobble together a handful of statements per year, scattered over a five-year period—most of which consist of general statements about security that have nothing to do with core case issues involving address book data or third party apps, and many of which appeared in locations (*e.g.*, technical journals, license agreements with apps developers, regulatory submissions, and rarely-viewed web pages) not likely to be viewed by a consumer. And in any case, multiple alleged "advertising campaign" statements only confirm that Apple prohibited the very conduct that is the subject of Plaintiffs' claims.

As before, Plaintiffs seek to salvage their misrepresentation claims by alleging "omissions," but the Court has already found that a manufacturer's obligations to disclose alleged product defects are confined to warranty obligations absent an affirmative misrepresentation or a safety issue. It is also undisputed that Apple disclosed, in its Privacy Policy (where consumers would naturally look for privacy-related information), the very information that Plaintiffs' claim was omitted, *i.e.*, that apps can collect device address book data. And, taking SAC allegations at face value, Plaintiffs and consumers were in all events well aware of the information purportedly "omitted" by Apple. For all of these reasons, Plaintiffs' misrepresentation claims fail.

Plaintiffs' remaining counts against Apple, for Conversion and Invasion of Privacy (Counts 1 and 2)—based on the theory that Apple "aided and abetted" the App Defendants' primary torts—fare no better. Under California law, aiding and abetting liability requires that a defendant had actual knowledge of the specific primary wrong and that the defendant substantially assisted commission of that wrong. On the knowledge element alone, Plaintiffs' allegations are fatally deficient—alleging "recklessness" and supplying no factual allegation that Apple *knew of* and decided to assist alleged unauthorized collection of user address book data.

Finally, pursuant to Sections 230(c)(1-2) of the Communications Decency Act ("CDA" or "Section 230"), Apple is immune from liability on all claims, to the extent those claims are premised on conduct other than an affirmative misrepresentation made by Apple and relied upon by Plaintiffs. This Court has already found that Section 230 immunity covers claims against Apple related to screening, testing app content, and providing development tools and guidelines. And while the Court also previously ruled that Plaintiffs' allegations permitted an inference that Apple was a content provider with respect to the offending content in this case—precluding a broader ruling of immunity—Apple asks the Court to revisit that ruling in light of the SAC and the expanded pleadings record, as well as recent decisional law on CDA immunity.

For all of these reasons, Apple respectfully requests that the Court dismiss each of Plaintiffs' claims against it—this time with prejudice.

II. PLAINTIFFS' ALLEGATIONS AND PROCEDURAL BACKGROUND

A. The Parties

The named Plaintiffs are 15 individuals who allege that they downloaded the App Defendants' apps to their Apple mobile devices, and that Defendants "caused" those apps to "secretly upload, store, and in some cases disseminate their personal and private address books … ." SAC ¶¶2, 139-232. Plaintiffs propose to represent a class of "[a]ll United States residents who purchased iDevices between July 10, 2008 and February 2012," and a subclass consisting of all putative class members who downloaded one of multiple popular third-party apps. *Id.* ¶233.

Apple manufactured the mobile devices allegedly purchased and used by Plaintiffs. *Id.* ¶¶1, 19. Users can download third-party software apps onto these devices through the Apple "App Store." *Id.*

¶39. Plaintiffs allege that before distributing any app to end users, Apple "conducts a review of all applications submitted for inclusion in the App Store" and "has sole discretion over the App approval process." *Id.* ¶¶44, 47. The App Defendants are the creators of the third-party apps that allegedly uploaded address book information from Plaintiffs' devices without consent. SAC ¶¶90, 93-138.

The SAC asserts all six of its counts against Apple: 1) Invasion of Privacy; 2) Conversion; 3) violations of California statutory False Advertising Law ("FAL"); 4) violations of California's Consumers Legal Remedies Act ("CLRA"); 5) Deceit, (Cal. Civ. Code § 1709 *et seq.*); and 6) violations of California's Unfair Competition Law ("UCL"). Plaintiffs assert two claims against the App Defendants: Count 1, Invasion of Privacy, and Count 2, Conversion.

B. Procedural History

The SAC represents Plaintiffs' fourth attempt to allege claims against Apple and follows this Court's dismissal of all claims against Apple asserted in the preceding Consolidated Amended Complaint ("CAC"). *See* May 14, 2014 Order re Motions to Dismiss ("MTD Order"). In the CAC, Plaintiffs asserted in substance the same claims they do here: They alleged that Apple "repeatedly represented that Apple's products are safe and secure, and that private information could not be accessed by third-party apps without the user's express consent." CAC ¶64. Plaintiffs sought to hold Apple liable for the App Defendants' alleged unauthorized uploads of address book data. *Id.* ¶128.

Before these cases were related and a consolidated complaint filed, Apple twice moved to dismiss claims filed by Plaintiff Pirozzi. Judge Gonzalez-Rogers granted Apple's first motion to dismiss. This Court then heard Apple's second motion to dismiss the Pirozzi complaint, and overruled it in part with respect to misrepresentation claims. In later ruling on Apple's Motion to Dismiss the CAC, however, the Court reconsidered and dismissed Pirozzi's (and the other Plaintiffs') fraud-based claims against Apple, because "Plaintiffs have failed to allege that any one of them saw any particular representation." MTD Order at 24-25. The Court also held that Plaintiffs had not avoided the requirement of pleading reliance: "Although Plaintiffs allege a long-term advertising campaign, they fail to do so with the level of detail that has led other courts to allow such claims to proceed." *Id.* at 31-32.

The MTD Order also included rulings that: (1) copying of Plaintiffs' address books did not constitute an injury, and Plaintiffs thus lacked standing to assert conversion or trespass; (2) the Court

"need not await further discovery before addressing Apple's CDA argument"; (3) certain of Plaintiffs' allegations against Apple involve conduct "protected by the CDA," including provision of a software development kit, promulgation of review guidelines, review of apps submitted to the App Store, and enforcement of guidelines; and (4) at that "juncture," the Court could not conclude all of Apple's alleged conduct at issue to be protected by the CDA, because the CAC pled "sufficient conduct to classify Apple as an 'information content provider.'" *Id.* at 16, 21-23 & n.12. The Court dismissed all counts against Apple with leave to amend; the SAC followed.

C. Allegations Against Apple in the Second Amended Complaint

1. The Alleged Misrepresentations

Plaintiffs allege that over a five-year period, Apple "consciously and continuously misrepresented its iDevices as secure, and that the personal information contained on iDevices—including, specifically address books—could not be taken without their owners' consent." SAC ¶3. Apple allegedly "consistently and deliberately failed to reveal its products' security flaws to consumers." *Id.* ¶4. As a result of Apple's "continuous and deliberate media campaign," Plaintiffs allegedly formed a particularized "expectation" that Apple devices were secure with respect to address book data. *Id.* ¶18.

On inspection, Apple's "continuous and deliberate media campaign" consists of an assortment of licensing agreements between Apple and third party developers, product user manuals, scientific and technical journals, Congressional testimony, regulatory submissions, and other materials that can hardly be described as consumer advertising. *E.g.*, SAC ¶¶76x, xi, xii, xviii; 77ii, iii, v; 78i-vi. The SAC also invokes blog and social media entries, news reports, and statements from Apple's website. *E.g.*, *id.* ¶76. Notably, a number of the challenged statements come not from Apple, but rather from third parties writing *about* Apple. What is more, the alleged statements share little in common, except that many happen to mention the words "security" or "privacy." Only a handful even arguably implicate address book security related to third-party applications. To the contrary, the vast majority of the so-called "campaign" consists of generalized statements about security or privacy, or discussions of unrelated security features, including password protection, corporate network security, and computer viruses. *Id.* ¶¶70, 71, 76iv, x-xii, xv, xviii, xxi, xiii; 150iii, 163iii, 170iii, 199iii, 212iii; Exs. G, I, K, N, Q.

Notably, not one of the 15 Plaintiffs claims to have seen or heard *any* of the specific statements alleged to comprise Apple's media campaign. Rather, they allege, for example, that they were exposed to "numerous [unspecified] advertisements and reports about Apple's safety and security" in "traditional and non-traditional media." *Id.* ¶¶144i, 150i, 156i, 163i, 170i, 176i, 182i, 187i, 193i, 199i, 205iv, 212i, 225i, 232i. To the extent that Plaintiffs purport to offer additional information about what they saw, it is equally conclusory: *e.g.*, attending or seeing product conferences or launch events, media reports, television, in-store advertisements, or Apple's website. No Plaintiff identifies specific misstatements he saw or heard, who made them, or when they were made. *Id.* ¶¶144i, 150iii, 163i, 170i, 187i, 193i.

2. Apple Disclosures

Plaintiffs complain that Apple failed to disclose that applications could collect data in user address books. SAC ¶¶143, 149, 155, 162, 175, 181, 187, 193, 198, 204, 211, 217, 224, 231. But Apple's Privacy Policy—to which all users of the App Store must agree *before* downloading any App—discloses that third-party apps may collect information such as contact and location data from their devices, and expressly directs users to the developers to learn more about the privacy practices of their third-party apps. Specifically, Apple's Privacy Policy provides:

> Our products and services may also use or offer products or services from third parties – for example, a third-party iPhone app. Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to lean about the privacy practices of those third parties.

Request for Judicial Notice ("RJN"), Ex. G at 4; *see also* Dkt. No. 147-1.

What is more, Plaintiffs repeatedly allege that the information allegedly omitted by Apple was widely known. According to Plaintiffs, Apple repeatedly disclosed the challenges associated with creating a secure platform that also made available third-party apps,[1] sought to improve security through both contractual and technical means, and took action whenever it learned that apps violated its policies or evaded its technical protections. For example, Plaintiffs allege that in July 2008, media reports revealed that the Aurora Feint App—distributed to hundreds of thousands of Apple device users—was transmitting users' address book data to the developer's servers without consent, leading Apple to delist

[1] Apple acknowledged: "We're covering new ground and doing things that had never been done before. Many of the issues we face are difficult and new, and while we may make occasional mistakes, we try to learn from them and continually improve." *See* RJN Ex. F at 2.

the App. CAC ¶219.[2]

In short, according to Plaintiffs, this information—all of which was supposedly part and parcel of the alleged Apple media campaign—was well known.[3] Indeed, "every representation, promise, hint, or even rumor about Apple's products quickly spreads through traditional and non-traditional media to *virtually the entire population of this country*." SAC ¶34 (emphasis added). Plaintiffs' own allegations thus set forth how consumers knew throughout the alleged class period that certain apps could (and had) collected private information on Apple mobile devices—including address book information.

III. ARGUMENT

A. Plaintiffs' Misrepresentation Claims—Counts 3, 4, 5, and 6—Fail

Under Rule 8, Plaintiffs must plead *facts* sufficient "to state a claim for relief that is plausible on its face." MTD Order at 8 (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). This Court has already found that Plaintiffs' misrepresentation claims sound in fraud. *Id.* at 23. Those claims are accordingly subject to Rule 9(b) and must include the "time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007). Plaintiffs are required to allege specific facts setting out "what is false and misleading about a statement, and why it is false." *Id.*[4]; *see also Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (requiring the "who, what, when, where, and how of the misconduct charged … what is false or misleading about a statement, and why it is false") (citations and internal quotations omitted).

Critically here, Plaintiffs must allege that they relied on identified misrepresentations. The mere

---

[2] In the SAC, Plaintiffs allege Aurora Feint as an example of Apple's "concealed" knowledge of security flaws. *See* SAC ¶83. In their CAC, however, Plaintiffs specifically alleged that the issue came to Apple's attention only following "media reports." CAC ¶219. Plaintiffs drop the "media reports" allegation from the SAC, presumably because it undercuts their argument that the alleged security defects were not public knowledge. *See* SAC ¶83. The CAC allegation, however, remains part of the pleadings record for the Court to consider on this Motion. *See* infra at III.C.

[3] Additional examples include Plaintiffs' allegations that: (1) Apple disclosed a security flaw in the iPhone "that gives unauthorized access to contacts and e-mails" and acknowledged: "We are aware of this bug" (SAC ¶76ix), and (2) Apple terminated the Google Voice App in August 2009 because the App had transferred iPhone users' entire Contacts database to Google's servers (*Id.* ¶84, RJN Ex. F at 2).

[4] Plaintiffs allege a claim for Deceit under California Civil Code Sections 1709 *et. seq.* These sections codify California common law actions for fraud and deceit. *Small v. Fritz Cos., Inc.*, 30 Cal. 4th 167, 172 (2003). Rule 9(b) pleading standards accordingly apply.

fact that Plaintiffs held an "expectation" is insufficient to allege fraud. Rather, Plaintiffs must identify individual representations and the "specifics" of their reliance upon such statements. MTD Order at 34 (dismissing CAC misrepresentation claims because Plaintiffs "failed to plead with particularity the specific representations upon which they relied"); *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 924 (N.D. Cal. 2012). The requirement is the same for other claims sounding in fraud, including claims under the UCL, FAL, and CLRA. *See* MTD Order at 34 (dismissing UCL, FAL, CLRA and negligent misrepresentation claims in the CAC); *In re iPhone 4S Consumer Litig.*, 2013 WL 3829653, at *12-13 (N.D. Cal. July 23, 2013) (dismissing UCL, FAL, CLRA, and common law fraud claims; plaintiffs did not specify "*particular* commercials, presentations or portions of the website" that "*each* was exposed to and relied upon") (emphasis added).[5]

1. The SAC fails to plead reliance on any particular misrepresentation.

Like its predecessor, the SAC fails to link any particular Plaintiff with any alleged misrepresentation. None of the named Plaintiffs claims to have read or heard *any* of the statements identified in the paragraphs 76-78 of the SAC. Instead, Plaintiffs say they were "exposed" to Apple's media campaign. But this is insufficient to allege reliance on any particular representation. *See Haskins v. Symantec Corp.*, 2014 WL 2450996, at *1 (N.D. Cal. June 2, 2014) (Tigar, J.) (dismissing UCL and CLRA claims under 9(b) where plaintiffs allege only that they "'relied' on a very long list of representations, and [were] 'exposed to' those representations").

Nor do the SAC's remaining allegations provide facts to satisfy this pleading requirement. Five Plaintiffs allege only that they saw or heard "numerous advertisements and reports about Apple's security and safety" in "traditional and non-traditional media" (SAC ¶¶156i, 176, 182i, 205iv, 225i) (Carter, Green, Hodgins, Moses and Sandiford). But "cursory allegations" that Apple "repeatedly represented that [its] products are safe and secure," are insufficient to plead a fraud-based claim. MTD Order at 32. The remaining Plaintiffs fare no better:

- Beuershausen, Biondi, Dean, Dennis-Cooley, Hoffman, King, Mandalaywala, Paul, and Varner claim to have viewed (unspecified) television advertisements, "statements and news reports," press releases, or "technology media sources," or to have attended or viewed unidentified

[5] *See also In re Facebook PPC Adver. Litig.*, 2010 WL 3341062, at *12 (N.D. Cal. July 23, 2013) (dismissing UCL claim where plaintiffs failed to identify representations reviewed with particularity); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1027 (N.D. Cal. 2012) (dismissing FAL claim with prejudice because plaintiffs never alleged that they had read alleged false representation).

conferences or product release events. SAC ¶¶144i, 150iii, 163i, 187i, 193i, 199i, 212i, 232i.

- Dennis-Cooley and Varner claim to have heard presentations by Stephen Jobs, but do not specify what presentation they heard, what Mr. Jobs said, or whether they saw any of the specific presentations identified as part of the alleged "media campaign." *Id.* ¶¶163i, 232i.
- Pirozzi says that she viewed Apple's website, unspecified in-store advertisements, and relied on Apple's reputation for security. *Id.* ¶218. These allegations are unchanged from the CAC (¶28), and fail for the same reasons.
- Beuershausen claims to have received a statement about "privacy" on an Apple invoice at some unspecified time prior to some unspecified purchase. *Id.* ¶144i.

These allegations do not establish *who* made the representations supposedly relied upon, *what* specifically the representation said, *when* the representation was made, or *why* it was false at the time it was made. *See Vess*, 317 F.3d at 1106; *see also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126 (9th Cir. 2009). Nor do Plaintiffs plead any facts to establish that any one of them justifiably relied on the alleged statements in forming any "expectation" that address book data was secure. *See also* discussion infra at IIIA.2.a.

2. The supposed "advertising campaign" does not salvage Plaintiffs' claims.

Plaintiffs seek to avoid reliance pleading requirements for at least their UCL and FAL claims by attempting to allege a "long-term advertising campaign" within the meaning of *In re Tobacco II*. *In re Tobacco II Cases*, 46 Cal. 4th 298 (2009). But Plaintiffs come up short. *First*, as a legal matter, *Tobacco II* "merely provides that to establish UCL standing, reliance need not be *proved* through exposure to particular advertisements; the case does not stand for, nor could it, a general relaxation of the *pleading requirements* under Rule 9(b)." *In re iPhone 4S Consumer Litig.*, 2013 WL 3829653, at *12 (emphasis added); *see also Herrington v. Johnson & Johnson Consumer Cos., Inc.*, 2010 WL 3448531, at *13 (N.D. Cal. Sept. 1, 2010); *In re Actimmune Mktg. Litig.*, 2009 WL 3740648, at *11-13 (N.D. Cal. Nov. 6, 2009), *aff'd* 464 Fed. Appx. 651 (9th Cir. 2011) (rejecting allegations that patients came to believe that a product was "efficacious" as a result of exposure to a marketing campaign, absent allegations of reliance on specific misrepresentations). Even had they sufficiently alleged a "long-term advertising campaign," Plaintiffs' failure to identify specific Apple representations on which they relied, under the rulings just cited,[6] would still be fatal to all of their misrepresentation claims.

[6] Precedent cited in text, including *In re iPhone 4S Consumer Litig.* and *Herrington*, compels the conclusion that Plaintiffs' fraud-based allegations would fail under Rule 9(b), regardless of whether Plaintiffs succeeded in pleading a long-term advertising campaign under *Tobacco II*. Although this Court sets out factors to consider in assessing whether *Tobacco II*'s long-term advertising campaign

Second, even assuming that the *Tobacco II* exception were to apply and excuse pleading particularized reliance for UCL and FAL claims, Plaintiffs fail to plead that Apple engaged in anything remotely resembling a *Tobacco II* campaign, and plainly flunk the six-factor test set out in this Court's MTD Order. The alleged Apple advertising was neither long-term nor extensive, consisting of disparate messages unrelated to the SAC's alleged core deception; the bulk of alleged communications comprised generic, truthful statements regarding security, irrelevant to Plaintiffs' claims.

a. Plaintiffs do not adequately allege exposure to the "campaign."

In dismissing the CAC, the Court held that "it is not clear that any of the plaintiffs were actually exposed to Apple's advertising campaign." MTD Order at 32. In response, the SAC baldly alleges that Plaintiffs *were* exposed. SAC ¶¶144ii, 150ii, 156ii, 163ii, 170ii, 182ii, 187ii, 193ii, 199ii, 205ii, 212ii, 225ii, 232ii. But merely mouthing the words is insufficient; Rule 9(b) requires *facts*. Not a single Plaintiff can identify even one representation on which he or she supposedly relied. No Plaintiff alleges that he or she ever heard anything about address book security, or "sandboxing" of one application from another, or the ability of applications to access and upload data stored in other applications.

Indeed, to the extent Plaintiffs recall *any advertisements* at all, they involve wholly unrelated issues: for example, Plaintiff Carter alleges that she recalls seeing or hearing something, from someone, at some point, to the effect that Apple products were "safe" because users had to input an Apple ID and password to access the App Store. SAC ¶156iii. Dennis-Cooley recalls advertisements about Apple's computers being safe from computer viruses. *Id*. ¶163iii. But such allegations fail to support an inference that Plaintiffs were exposed to an advertising campaign communicating that address book data could never be collected and used by third party applications.

b. The SAC fails to allege a long-term or extensive campaign.

The "advertising" statements alleged by Plaintiffs span a period of five years—a far cry from the "decades-long" campaign at issue in *Tobacco II*. Courts have deemed longer alleged campaigns insufficient. *See Haskins*, 2014 WL 2450996, at *2 (seven year campaign insufficient) (citing *Actimmune*, 2009 WL 3740648, at *13). What is more, multiple alleged Class Period purchases

exception should be applied in a particular case, Apple does not read the MTD Order to specifically reach (or disagree with) such precedent, requiring Rule 9(b) compliance in all events.

occurred substantially *less* than five years into the alleged "campaign." At the time of Plaintiffs' alleged Apple device purchases in 2007 or 2008, the "media campaign" consisted of a mere five statements spanning roughly a year. For 2009 purchases, it consisted of nine alleged statements made in the course of two years. This is not the stuff of a "long-term advertising campaign." *See id.* (advertising campaign lasting from 2006 to 2007 or 2008 insufficient); *Pfizer Inc. v. Super. Ct.*, 182 Cal. App. 4th 622, 633-34 (2010) (six-month campaign involving four television commercials insufficient).

Nor is the alleged campaign sufficiently "extensive." Plaintiffs assert that Apple spent "hundreds of millions" advertising its App Store in print and television commercials, RSS feeds, and website posts, SAC ¶¶67, 69, but say nothing about sums spent to disseminate the allegedly *false statements at issue*—thus failing to establish an "extensive" campaign. *See Delacruz v. Cytosport, Inc.*, 2012 WL 2563857, at **5, 9 (N.D. Cal. June 28, 2012) (allegation that Cytosport spent tens of millions advertising—internet, website, magazines, billboards, paid endorsements, agreements with academic institutions, tradeshows, other media outlets—insufficient to plead long-term advertising campaign).

Nor have Plaintiffs adequately alleged the frequency with which advertisements appeared. MTD Order at 32. Instead, Plaintiffs offer sweeping hyperbole that anything Apple said was "invariably reported by thousands of media outlets, dissected by pundits and bloggers, frequently posted on Apple's own website, and available on countless websites and social media platforms, and thus made available to virtually all potential customers." SAC ¶62. But Plaintiffs' "buzz marketing" allegations are conclusory and fail to plead *any* misrepresentation, let alone a misrepresentation by *Apple*.

A valid fraud claim requires a false statement *by* Apple. Plaintiffs instead seek to hold Apple liable for statements made *about* Apple. The SAC is replete with marketing jargon like "buzz marketing," "non-traditional media," or "earned media," all of which typically involve online content *posted by users or consumers*, often in social networking sites.[7] But that people talk *about* Apple does equate to a marketing campaign *by* Apple regarding third party app security. *See, e.g., Yordy v. Plimus, Inc.*, 2012 WL 2196128, at *5 (N.D. Cal. June 14, 2012) ("Under the FAL or UCL, a defendant's

[7] Plaintiffs do not bother to define these terms in their SAC, but "buzz marketing" and "earned media" clearly consist at least in part of statements by third parties, including online content distributed by consumers via Facebook posts, tweets, blogs, YouTube videos, Instagram, reviews, tweets, or online forum posts or social networking sites.

liability must be based on *his personal participation* in the unlawful practices and *unbridled control* over the practices that are found to violate section 17200 or 17500.") (emphasis added) (internal quotations omitted) (citing *Emery v. Visa Int'l Serv. Ass'n*, 95 Cal. App. 4th 952, 960 (2002)); *see also In re Jamster Mktg. Litig.*, 2009 WL 1456632, at *9 (S.D. Cal. May 22, 2009) (CLRA liability must be based on defendant's "participation or control in the alleged unlawful advertising scheme").

c. The SAC fails to identify false or actionable statements.

To invoke *Tobacco II*, Plaintiffs must attach a representative sample of the advertisements at issue and identify what, in particular, the defendant is alleged to have said, and how it was false. MTD Order at 29. But these Plaintiffs provide only a laundry list of Apple and third-party statements (SAC ¶¶76-78), never explaining what was supposedly false about them. Plaintiffs' theory appears to be that because certain third party apps allegedly uploaded address books, every Apple statement that mentioned the words "privacy" or "security," from 2007 onward, was false. As discussed, this facile assumption finds no support in either the text of the alleged statements or their surrounding context. And many of the alleged statements are not actionable because they are "generalized, vague, and unspecified assertions … upon which a reasonable consumer could not rely." *Rasmussen v. Apple, Inc.*, 2014 WL 1047091, at *9 (N.D. Cal. Mar. 14, 2014).

i. General statements about "security" and "privacy" are not actionable.

As evidence of the purported media campaign, Plaintiffs rely heavily on general statements about "security" and "privacy." *See, e.g.*, SAC ¶71 ("Your privacy is a priority at Apple, and we go to great lengths to protect it"); ¶76iv, Ex. D (iPhone is "secure and reliable"); ¶76xxiv ("Apple respects your privacy"). But these statements say nothing about address books or the ability of applications to collect data from other applications. None amounts to a guarantee that security breaches could never happen. To the contrary, Plaintiffs acknowledge that, as part of its alleged media campaign, Apple warned consumers of security defects that permitted "unauthorized access to contacts and e-mails," *id.* ¶76ix, and warned that third party applications might try to steal personal data, *id.* ¶76xiv, Ex. M.

Moreover, multiple alleged statements by Apple are not actionable because they do not make a "specific and measurable claim, capable of being proved false or of being reasonably interpreted as a statement of objective fact." *Rasmussen*, 2014 WL 1047091, at *9. "[A]dvertising which 'merely states

in general terms that one product is superior is not actionable.'" *Id.* *See also Minkler v. Apple, Inc.*, Case No. 5:13-CV-05332-EJD (N.D. Cal. August 20, 2014) (dismissing CLRA, FAL and UCL counts; "Plaintiff has failed to identify any specific statement by Apple that expressly indicates Apple Maps would always work flawlessly and without error") (citing *In re IPhone 4S Consumer Litig.*, 2014 WL 589388 (N.D. Cal. Feb. 14, 2014)).

In *Heartland Payment Systems*, for example, involving a credit information data breach, the court concluded that a representation that the defendant used "layers of state-of-the-art security, technology and techniques to safeguard sensitive credit and debit card account information" was non-actionable. *See In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 592 (S.D. Tex. 2011), *partially rev'd on other grounds, Lone Star Nat. Bank. N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013) (citing *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 119 (D. Maine 2009)). In so doing, the court held that it is unreasonable to expect perfect security, and therefore unreasonable to interpret the representation at issue as promising that no breach will ever take place. *Id.* Other courts have held similar security-related assertions to be non-actionable. *See Haskins*, 2014 WL 2450996, at *2 (rejecting as non-actionable Symantec representations that its product helped users "[s]tay protected," "detects and removes spyware," and "blocks spyware and worms automatically").

Applying these standards, many of the statements Plaintiffs rely on are not actionable, because they do not involve "specific and measurable" product characteristics. *See* SAC ¶¶76i, Ex. A ("It's got awesome security"); ¶76viii, Ex. H ("Your privacy is a priority at Apple, and we go to great lengths to protect it"); ¶76xiv, Ex M ("[Apple has] built a store for the most part that people can trust"); ¶76ii ("Apple takes the security of your personal information very seriously"); ¶76xxiii, Ex. U ("strong privacy protections for our customers" and "privacy and trust are vitally important"); ¶¶76xxv, xxvi ("Protecting customer privacy is a key feature of all App Store transactions").

ii. Other alleged statements do not support liability.

To the extent that Plaintiffs purport to identify other statements, they fail to allege what was false, misleading, or material.

Pre-App Store: Plaintiffs cite several general statements preceding the July 2008 launch of the

App Store, when Apple was exploring how to create such a store, but fail to allege how those statements—about the challenges relating to combining security with an open platform—were false.[8] Plaintiffs identify only a smattering of arguably relevant statements, discussing Apple's *plans* for the App Store and software designed by third-party developers. None mentioned address books, much less guaranteed their security. For example, Mr. Jobs acknowledged that opening Apple's platform to application developers posed security risks. SAC ¶76iii. In another alleged statement, Mr. Jobs allegedly said: "We *want* to take the best of both: reliability of the iPod, but the ability to run 3rd party Apps." *Id.* ¶76vi (emphasis added). This is a statement of future intent, not a guarantee. What is more, Mr. Jobs warned that the iPhone would be a "highly visible target" for malicious programs. *Id.* Ex. E.

Security in corporate networks and device passcodes: Other of Plaintiffs' allegations simply have nothing to do with Plaintiffs' alleged injury. For example, the SAC contains many allegations related to the security of corporate networks,[9] but no Plaintiff alleges that he or she bought an Apple device for use in a corporate network and, moreover, Plaintiffs never allege that any of these statements was false. Similarly, the SAC references putting passcodes on the device (citing a single sentence buried in a 217-page user guide)[10]—but again does not allege how the representation was false or how it relates in any way to whether third-party apps could collect data without user permission.

App Developer License Agreements and Guidelines: Plaintiffs repeatedly characterize contracts between Apple and third-party developers as part of an Apple media campaign targeted at consumers. SAC ¶¶76 xi, xii, xxviii. But as Plaintiffs elsewhere acknowledge, Apple intended these agreements to be private. *See id.* ¶53 ("Through the iOS Developer Program License Agreement, Apple further restricts information concerning the development process and prohibits developers from publicly

[8] For example, Plaintiffs challenge statements in an Apple Privacy Policy dating from 2007, but allege no facts to suggest that Apple did not in fact take "precautions" to safeguard user data. SAC ¶76ii (Ex. B). To the contrary, the SAC identifies several Apple precautions, including SSL encryption for App Store transactions, Apple ID and password requirements, and password protection on Apple devices. *E.g.*, Ex. B; ¶76x, 156iii. What is more, the challenged statement discusses *Apple's* treatment of customer information collected by *Apple*, not data collection by third party apps that did not then exist.

[9] iPhone "delivers secure access to corporate intranets" and corporate resources, and companies can "securely sync" (Ex. G); the iPhone can "securely access corporate services and protect data on the device" (Ex. K); corporate administrators can "securely manage any iPhone"; and, that as used in a corporate network, iOS 4 provided "improvements in security," "better data protection," and was "even more secure" than its predecessor operating system. Exs. N, Q.

[10] SAC ¶76x, Ex. I; *see also id.* at ¶76xv, Ex. N ("iPhone OS4 now provides the option to set a longer, more complex passcode, making the iPhone and its data even more secure").

discussing Apple's standards for App development"). In any event, the Developer Agreements do not assist Plaintiffs—they demonstrate that Apple repeatedly *prohibited* developers from collecting personal data without permission. *See* discussion, *infra* at III.D.3.

While Plaintiffs purport to identify two public statements indicating that "Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used" (SAC ¶76xxi, xxiii) and refer elsewhere to developer guidelines prohibiting apps from collecting user data without user permission (*id.* ¶¶47, 87), these statements were aimed at developers, not consumers. They not only are not false but instead comprise (or reflect) binding contractual provisions included in App Developer agreements banning developers from doing what the App Defendants are alleged to have done.

Sandboxing: Plaintiffs identify a grand total of five statements regarding "sandboxing." Putting aside Plaintiffs' failure to allege facts explaining how the "sandboxing"-related statements cited relate to apps collecting user data without advance permission, the SAC fails to allege how the statements were part of an advertising campaign or how they were false. Two of the five statements appear in scientific journals; the third was made by an Apple development leader at an Apple shareholder meeting. Neither journal remotely asserted that sandboxing provided a guarantee of security for information stored on mobile devices. *Id.* ¶¶77ii Ex. Z, 77v Ex. CC. And while Plaintiffs also invoke a presentation by Mr. Jobs, he acknowledged that sandboxing might be imperfect: "[W]e think we've put in good safeguards where, if we miss something, we'll be alerted to it real fast by users, and we'll just turn off the spigot so no more users have problem [*sic*]." *Id.* ¶77i. Again, the cited sandboxing statements do not support a plausible inference of a long-term advertising campaign.

d. The alleged statements did not comprise a single set of messages.

To qualify as a "long-term advertising campaign," the alleged statements must be "similar enough to be considered as part of one campaign, or the delivery of a single message or set of messages, rather than a disparate set of advertising content published in the ordinary course of commerce." MTD Order at 30. Plaintiffs fail to allege a "single set of messages." As discussed above, SAC-alleged statements address security or privacy in a wide range of contexts—including corporate network applications, App Store transactions, device passcodes, storage, location data, and others. Simply put,

only a handful of alleged statements even arguably address security as it relates to address books; the vast majority address different, widely varying topics. Rather than advertising to prospective consumer purchasers, the statements cited were intended for different audiences: prospective business users, Apple users who had already purchased devices, investors, and federal regulators and members of Congress. And many of the alleged statements came from *third parties* with radically differing viewpoints. Plaintiffs have not alleged a unitary advertising campaign with a single set of messages.

e. The SAC fails to plead when and how Plaintiffs were exposed to the alleged campaign.

"In the absence of specific misrepresentations, a complaint subject to Rule 9(b)'s requirements should plead with particularity, *and separately*, when and how each named plaintiff was exposed to the advertising campaign." MTD Order at 30. "It is not enough merely to allege that Plaintiffs 'viewed Apple's website, saw in-store advertisements, and/or were aware of Apple's representations … ." *Id.* at 33. The SAC provides none of the required details, alleging only that Plaintiffs were exposed to "numerous advertisements" in "traditional and non-traditional media" at unspecified times prior to their purchases. *E.g.*, SAC ¶¶150, 156, 163, 170, 176. These allegations are virtually indistinguishable from ones already rejected by this Court. Further, they fail to satisfy the Court's "when and how" test, which "ensures that the advertisements at issue are representations that consumers were likely to have viewed, as opposed to representations that were isolated or more narrowly disseminated, such as statements buried on a rarely-viewed webpage, or made on an investor phone conference." MTD Order at 31. In another recent decision, this Court dismissed claims predicated on an "advertising campaign" that rested on "press releases and industry documents that an average consumer would be unlikely to read," holding that "[t]he only representations it is reasonable to assume Plaintiff was exposed to appeared in popular media such as magazines and websites." *Haskins*, 2014 WL 2450996 at *2.

Here, the alleged campaign consists largely of statements that no reasonable consumer was likely to view—indeed, none of the Plaintiffs claims to have viewed them—including Apple license agreements with third-party developers (SAC ¶¶76xi, xxii, xxviii); corporate press releases/articles (¶76iv, ix, xv, xxv); rarely viewed webpages (¶xx)[11]; scholarly articles (¶¶77ii, v); Apple shareholder

[11] Plaintiffs rely on a statement allegedly posted on Apple's website in July 2010 stating that "All Apps run in a safe environment, so a website or App can't access data from other Apps." SAC ¶76xx. As

meetings (¶77iii); and regulatory submissions, Congressional testimony, and a "sworn declaration" (¶¶78i-vi). Others involve Apple product manuals (¶76x, Ex. I), typically read *after* a product purchase. These statements—which comprise a substantial portion of the total alleged statements—furnish no support for the alleged "media campaign."

3. Plaintiffs have not alleged any actionable omission.

Plaintiffs attempt to avoid reliance pleading requirements in a second way: by recasting the alleged misrepresentations as omissions. Thus, Plaintiffs claim that Apple failed to disclose that applications could collect data in user address books. *See* Section II.C.2. But the SAC pleads no facts to suggest that Apple 1) actively concealed security defects from Plaintiffs, 2) had exclusive knowledge of material facts not known to Plaintiffs, or 3) otherwise had any duty to disclose security defects. For all of these reasons, Plaintiffs' omissions claims fail.

The omission claims are barred by applicable product warranties. "A manufacturer's duty to consumers is limited to its warranty obligations absent either an affirmative misrepresentation or a safety issue." MTD Order at 33-34; *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1141 (9th Cir. 2012). Absent a safety issue, an omission is not actionable unless the alleged defect—here, uploading of Plaintiffs' address book information—*actually manifested* within the warranty period. *See Rasmussen*, 2014 WL 1047091, at *9.

This Court dismissed the CAC omission claims on the ground that Plaintiffs failed to allege when they purchased their Apple devices, when the alleged defects arose, what kind of warranty Apple provided, the terms of the warranty, and the warranty's duration. MTD Order at 34. The SAC still omits critical details. Plaintiffs now allege that Apple provided a limited one-year warranty, but fail to state the warranty terms. Indeed, the only warranty language relevant to the alleged security defects—that contained in Apple's iOS Software Licensing Agreement ("SLA")—expressly "DISCLAIM[S]

---

the Court will recall, this statement was the subject of extensive prior briefing, Dkt. 395 at 6-7, 27-28, and the Court dismissed prior claims in part because no Plaintiff alleged having reviewed the statement, which appears on one page of Apple's many-page website. MTD Order at 25. Simply recasting the single, isolated statement as part of a long-term advertising campaign is insufficient, as is Plaintiffs' mantra (recited without the support of factual allegations) that this and other statements by Apple (and others) were "widely disseminated … through the mainstream and non-traditional media." Plaintiffs have failed to heed the Court's admonition that they must plead specific facts showing that an alleged false statement appeared where a reasonable consumer would likely see it. *Id*. at 33.

ALL WARRANTIES, stating that the iOS is provided "AS IS" and "WITHOUT WARRANTY OF ANY KIND." RJN Exs. A-E at ¶7. Further, the SLA expressly disclaims liability or responsibility for "any aspect" of third-party apps. *Id.* Ex. A at ¶5(c), Exs. B-E at ¶5(d). Because Apple did not warrant protection against the activities of third-party application developers, it had no obligation to "disclose" the possibility that third-party Apps would upload address books.

Plaintiffs also fail to allege facts establishing that their address books were actually uploaded during the warranty period. Plaintiffs first say that the defects "were inherent in the products and existed at the time of the purchase and at all times thereafter" and were "present from the outset." SAC ¶291. But the requirement is for manifestation of the defect during the warranty period, and courts routinely reject Plaintiffs' "latent defect" theory. *See Rasmussen*, 2014 WL 1047091, at *9; *see also Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 831-32 (2006). Alternatively, Plaintiffs allege baldly, with no supporting facts, that defects arose during the warranty period. Because Plaintiffs offer only "naked assertions … devoid of further factual enhancement," the allegations cannot be credited. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 557).

Apple did not conceal but instead disclosed the relevant information. Plaintiffs fail to plausibly plead an omission, much less active concealment, because judicially noticeable documents confirm that Apple *did* disclose that apps can access certain user data on its devices—including contacts. Specifically, Apple's Privacy Policy states that Apple's "products and services may … use or offer products or services from third parties—for example, a third-party iPhone app," and that those third parties may collect information, including "such things as location ***data or contact details***." RJN Exs. G at 4. And as noted, the SLA included a corresponding disclaimer of liability with respect to third-party apps. *See id.* Ex. A at ¶5(c), Exs. B-E at ¶5(d). Because Apple disclosed precisely the information that Plaintiffs say was omitted, the omissions claims must be dismissed. *See, e.g.*, *Fabozzi v. StubHub, Inc.*, 2012 WL 506330, at *6 (N.D. Cal. Feb. 15, 2012) (dismissing with prejudice UCL fraud claim based on alleged omission of ticket pricing information where the defendant's website "effectively discloses the information Plaintiff alleges it conceals); *Birdsong v. Apple, Inc.*, 590 F.3d

955, 961 (9th Cir. 2009).[12]

Apple did not have exclusive knowledge of material facts. Plaintiffs claim that they were unaware that third-party applications *could* upload, or had uploaded, address book information. SAC ¶80. To the contrary, Plaintiffs say this information was long openly discussed and transmitted widely (*id.* ¶34), in prominent media publications, (*e.g.*, *Wall Street Journal*, ¶76xxiii, Ex. U), and scientific journals (¶¶77ii, v, Exs. Z, CC), and by Apple representatives (¶76ix). Because Plaintiffs allege that the public already knew the information that Apple supposedly failed to disclose, Plaintiffs' omissions claims fail. *See, e.g.*, *Herron v. Best Buy Co, Inc.*, 924 F. Supp. 2d 1161, 1175 (E.D. Cal. 2013) (failure to allege defendant had exclusive knowledge of testing problems where testing protocol disclosed and third party published criticism of protocol prior to plaintiff purchase). Plaintiffs' omission theory cannot salvage their failed misrepresentation claims.

B. Apple Did Not Aid and Abet Any Invasion of Privacy or Conversion: Counts 1 and 2 Must Be Dismissed.

SAC Counts I and II for invasion of privacy and conversion fail as a matter of law. Those claims rely solely on a theory that Apple aided and abetted the App Defendants in their invasion of Plaintiffs' privacy and conversion of Plaintiffs' property. Plaintiffs tried and failed in the CAC to allege aiding and abetting as a separate count against Apple, CAC ¶¶809-12; MTD Order at 37-38; they fare no better as now alleged.

1. Plaintiffs' allegations of aiding and abetting are inadequate; both Count 1 and Count 2 against Apple fail on that basis.

Plaintiffs' Invasion of Privacy and Conversion claims fail, because the SAC contains no meaningful allegations that Apple knew about the App Defendants' alleged wrongful actions and consciously chose to assist them. Such allegations are required under California law. *Casey v. U.S. Bank Nat'l Ass'n*, 127 Cal. App. 4th 1138, 1144 (2005) (aiding and abetting liability permissible only if defendant "knows the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other to so act"; liability will only be imposed when the defendant "had actual knowledge of the specific primary wrong the defendant substantially assisted") (internal quotations and

[12] Under Rule 8, the Court "need not accept as true conclusory allegations that are contradicted by documents referred to in the complaint." *Colony Cove Props., LLC v. City of Carson*, 640 F.3d 948, 955 (9th Cir. 2011) (citing *Iqbal*, 556 U.S. 662 (2009)).

citations omitted); *Howard v. Super. Ct.*, 2 Cal. App. 4th 745, 749 (1992) ("[A]iding and abetting … requires a defendant to reach a conscious decision to participate in tortious activity for the purpose of assisting another in performing a wrongful act."); *see also In re First Alliance Mortg. Co.*, 471 F.3d 977, 993 (9th Cir. 2006) (citing *Casey*, 127 Cal. App. 4th at 1144). Instead, these Plaintiffs allege only that Apple "knowingly and/or recklessly permitted the unauthorized access and collection of Plaintiffs' and class members' private address books." SAC ¶250; *see also id.* ¶266.[13]

To begin, an allegation of reckless conduct—which is all Plaintiffs' allegation in the alternative amounts to—is insufficient to support a cause of action for aiding and abetting. *See Resolution Trust Corp. v. Rowe*, 1993 WL 183512, at *10 (N.D. Cal. Feb. 8, 1993) (rejecting argument that liability for aiding and abetting common law torts under California law can be established by evidence that defendant was reckless). But even if Plaintiffs had alleged the elements correctly, their *conclusions* must be disregarded, because they allege *no facts* supporting the necessary conclusion of knowing assistance. *Iqbal*, 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."); *Twombly*, 550 U.S. at 555.

In *Facebook, Inc. v. MaxBounty, Inc.*, 274 F.R.D. 279, 281 (N.D. Cal. 2011), for instance, Facebook complained that advertisers engaged in fraud by creating Facebook pages that lured users with promises of special offers, but led them to spam their Facebook friends and then withheld the special offer unless users signed up for subscription services from third-party websites. Facebook sought to hold advertising company MaxBounty liable for aiding and abetting that fraud, alleging that defendant knew "its affiliates are creating misleading Facebook pages and aids and abets this activity by providing technical support, suggestions for Pages, and financial incentives to affiliates." *Id.* at 285. The court dismissed the claim because "[t]hese allegations merely provide a 'formulaic recitation of a cause of action' and lack factual support." *Id.* (quoting *Twombly*, 550 U.S. at 555).[14]

[13] With respect to whether Apple substantially assisted any invasion of privacy, the focus must be on whether Apple substantially assisted the *unauthorized* access or copying of Plaintiffs' address books. For the reasons explained below in discussion of Apple's CDA defense, Plaintiffs have not alleged facts to support a plausible inference of such substantial assistance. *See infra* at III.D.3.

[14] *See also, e.g., Lintz v. Bank of Am., N.A.*, 2013 WL 5423873, at *9 (N.D. Cal. Sept. 27, 2013) (aiding and abetting allegation that defendant "knew or should have known" of another's wrongful conduct held insufficient); *Schulz v. Neovi Data Corp.*, 152 Cal. App. 4th 86, 97 (2007) (allegations concluding that defendants "knew of [] unlawful operations but knowingly and intentionally aided and abetted" them insufficient).

Plaintiffs' conclusory (and qualified) assertions concerning Apple's knowledge are indistinguishable from those rejected in *Facebook* and *Lintz.* As to each app identified in the SAC, Plaintiffs allege only that Apple "learned or *should have learned* of the App's malicious, prohibited features" when it reviewed the app before release in the App Store. SAC ¶¶93, 99, 104, 110, 114, 118, 122, 126, 130, 134.[15] The SAC provides no facts that would make plausible the conclusion that Apple *actually learned* of wrongful conduct by any of the App Defendants, and chose to further that conduct. To the contrary, the SAC cites two instances in which Apple removed apps from the App Store when it learned that they transmitted users' information without advance permission. *Id.* ¶¶83-84. The SAC also alleges that Apple's policies prohibit apps from collecting user data without user permission and that Apple put in place technical safeguards to prevent such conduct. *See infra* at III.D.3.

Therefore, Plaintiffs' only factual allegations concerning Apple's knowledge of the allegedly tortious conduct actually undermine any conclusion that Apple knew of apps collecting user address book data without consent.[16] The SAC thus fails to plausibly allege that Apple knew of and intentionally aided any invasion of privacy or conversion of users' contacts data. *See, e.g., Shkolnikov v. JPMorgan Chase Bank*, 2012 WL 6553988, at *14 n.6 (N.D. Cal. Dec. 14, 2012) (conclusory allegation implausible where contradicted by other facts alleged); *Bowes v. Christian Record Servs.*, 2012 WL 1865712, at *6 (C.D. Cal. May 21, 2012) (same).

[15] As to Path, the SAC further alleges "[o]n information and belief" that Apple "knew that Path was uploading consumers' address books." SAC ¶106. To reach that conclusion, Plaintiffs start with the allegation that Apple is a "joint-venturer in the iFund venture capital fund and mentoring program" and that "Path is an iFund company," then pile on a series of allegations "on information and belief" that Apple provided guidance to Path, including mentoring as to its app. *Id.* That Apple and Path are both involved in iFund, if true, does not plausibly support a conclusion that Apple specifically "mentored" Path on its app, let alone that Apple knew that Path's app was uploading Apple users' address books. Moreover, the allegation—because it is made on information and belief—should be rejected because it is unsupported by alleged facts that would make it plausible. *Vivendi SA v. T-Mobile USA Inc.*, 586 F.3d 689, 694 (9th Cir. 2009) (finding allegations based "upon information and belief" insufficient, where no further facts were alleged); *Solis v. City of Fresno*, 2012 WL 868681, at *8 (E.D. Cal. Mar.13, 2012) ("In the post-*Twombly* and *Iqbal* era, pleading on information and belief, without more, is insufficient to survive a motion to dismiss for failure to state a claim.").

[16] The allegation that Apple learned or should have learned *during the app review process* that apps uploaded user contacts data without permission is obviously inconsistent with the allegation that Apple itself developed the contacts-uploading functionality that Plaintiffs complain of. SAC ¶¶44-46. *See infra* at III.D.3.

2. Plaintiffs lack standing to assert a Conversion claim and cannot make out the necessary elements in any event.

The Court dismissed Plaintiffs' prior conversion claim against Apple for "lack [of] Article III standing based on any injury to their property rights in their address books." MTD Order at 16. In so doing, the Court reviewed and relied on numerous cases concluding that some abstract reduction in the value of a plaintiff's personal information from alleged unauthorized third party access is not cognizable injury. *Id.* at 39-40. The Court concluded that Plaintiffs here "have failed to allege any details concerning their argument that their address books' value was diminished by the App Defendants' conduct." *Id.* at 40. That failure persists. Plaintiffs allege they have the right to sell or license their address books, which they allege have "commercial value." SAC ¶¶58-59, 258-259. But there are still no allegations that any of them ever tried to sell or license that data or that, if they did, the commercial value of any Plaintiff's address book was diminished because of any App Defendant's access.

That is not surprising, as Plaintiffs are still in possession of their address books and can presumably extract whatever economic value ever existed. Their ongoing possession of their address books is yet another reason why Plaintiffs' conversion claim fails. To state a claim for conversion, the property at issue "must be capable of exclusive possession or control." *Kremen v. Cohen,* 337 F.3d 1024, 1030 (9th Cir. 2003). Personal information is not capable of exclusive control and therefore cannot be converted. *See Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *17 (N.D. Cal. Mar. 26, 2013) (courts are reluctant to find personal information is a form of personal property for conversion purposes, because "it is difficult to see how this broad category of information is capable of exclusive possession or control") (quoting *In re iPhone Application Litig.* ("*In re iPhone II*"), 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012); *In re iPhone II*, 844 F. Supp. 2d at 1074-75 (rejecting conversion claim relating to collection of consumers' "personal information" where plaintiffs could not show Apple held "exclusive possession or control" of the data); *Hernandez v. Path, Inc.*, 2012 WL 5194120, at *7 (N.D. Cal. Oct. 19, 2012) (dismissing conversion claim because plaintiff did not allege wrongful dominion of the property, only copying).

As this Court noted in dismissing Plaintiffs' previous attempt at stating a conversion claim: "In cases where the alleged converter has only a copy of the owner's property and the owner still possesses

the property itself, the owner is in no way being deprived of the use of his property. The only rub is that someone else is using it as well." MTD Order at 40, n.22 (quoting *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d 300, 304 (7th Cir. 1990). Even if personal data could be converted, Plaintiffs still have their copies of that data and, therefore, for purposes of a conversion claim they have not been deprived of possession of anything or otherwise injured. Accordingly, Plaintiffs' conversion claim fails for the additional reason that they cannot allege the required element of damage. *See, e.g.*, *L.A. Fed. Credit Union v. Madatyan*, 209 Cal. App. 4th 1383, 1387 (2012) (listing elements of a conversion claim).[17]

C. Plaintiffs Do Not Have Standing To Seek Injunctive Relief Against Apple.

Standing for prospective injunctive relief requires a plaintiff to allege that "he has suffered or is threatened with a 'concrete and particularized' legal harm … coupled with 'a sufficient likelihood that he will again be wronged in a similar way.'" *Bates v. United Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983)). That, in turn, requires a plaintiff to allege a "real and immediate threat of repeated injury." *O'Shea v. Littleton*, 414 U.S. 488, 496 (1974). "[P]ast wrongs do not in themselves amount to [a] real and immediate threat of injury necessary to make out a case or controversy." *Lyons*, 461 U.S. at 103.

These Plaintiffs cannot seek injunctive relief against Apple, because no realistic threat exists that the complained-of conduct is ongoing or will be repeated. First, as the Court previously noted, Plaintiffs have alleged that Apple remedied alleged gaps in its privacy protection. MTD Order at 39; CAC ¶120. Indeed, Plaintiffs claimed credit for the development. CAC ¶120 ("After the filing of this lawsuit … Apple released version 6 of its iOS. This iOS update included a Privacy setting that discloses what apps requested access to a user's Contacts app … ."). Those allegations were removed

[17] A claim for intrusion also fails as a matter of law where the injury is insubstantial: "If the undisputed material facts show … an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 40 (1994). To be sure, in its MTD Order, this Court determined that assessment of the offensiveness of unauthorized address book copying was best left to a jury. MTD Order at 46. But since that ruling, yet another Northern District court has held as a matter of law on the pleadings that the disclosure of specific user data to third parties did not rise to the offensiveness level required to state an invasion of privacy claim. *In re Google, Inc. Privacy Policy Litig.*, — F. Supp. 2d —, 2014 WL 3707508, at *1, 12 (N.D. Cal. July 21, 2014) (transfer of personal identifying information, including *browsing history and search queries*, failed to state a claim.) Nothing in the SAC suggests that the data at issue in this case—address book information regarding third parties—is more sensitive than a person's own location or the internet content a person has searched. If this Court were inclined to revisit this issue, strong support exists for a ruling that these Plaintiffs' allegations do not plead the requisite level of offensiveness.

from the SAC, which omits mention of Apple's steps to augment user privacy protections. Instead, the SAC alleges, inconsistently, that "Apple's foregoing misconduct is ongoing, and unless restrained by this Court, is likely to recur." SAC ¶281. But because they are contradicted by earlier allegations, the latest allegations are implausible and should not be accepted as true. *See, e.g.*, *Smith v. Wilt*, 2013 WL 5675897, at *4 n.5 (N.D. Cal. Oct. 17, 2013) (removal of facts present in an earlier complaint rendered current allegations "simply *not plausible*") (emphasis added); *Fasugbe v. Willms*, 2011 WL 2119128, at *5 (E.D. Cal. May 26, 2011) (collecting cases and concluding that "court may properly consider the plausibility of the [amended complaint] in light of the prior allegations"); *Stearns v. Select Comfort Retail Corp.*, 763 F. Supp. 2d 1128, 1145 (N.D. Cal. 2010) (same).

Second, regardless of Plaintiffs' prior pleading, an assertion that Apple's conduct is ongoing is unsupported by any *facts* alleged in the SAC. Plaintiffs list a variety of statements about privacy they seek to attribute to Apple, but none of them was made in the past two years. *See* SAC ¶¶76-78. Nor do Plaintiffs identify any incidents of unauthorized upload of address book data (or any other user data) in the past two years. For this reason too, Plaintiffs' allegation that Apple's conduct is "ongoing, and … likely to recur" cannot be accepted as true. *Twombly*, 550 U.S. at 554-55.

Finally, and more particularly, Plaintiffs lack standing to seek an injunction preventing Apple from making future misleading statements, because they do not claim they intend to buy any more iPhones, iPads, or iPod Touches. To the contrary, they claim that they "would not have purchased the iDevices for the retail price paid *or at all* had they known of the true facts." SAC ¶278. Now aware of the alleged facts in the SAC, Plaintiffs face no threat of repeated injury from Apple statements about the security of its devices. Multiple district courts in this Circuit have reached the conclusion that a plaintiff, seeking to enjoin a manufacturer in connection with alleged misleading statements about a product the plaintiff already purchased, must "allege that he intends to purchase the products at issue in the future," *Rahman v. Mott's LLP*, 2014 WL 325241, at *10 (N.D. Cal. Jan. 29, 2014), and that claims for injunctive relief unsupported by such allegations should be dismissed for lack of Article III standing. *Id.*; *see also Burns v. Tristar Prods., Inc.*, 2014 WL 3728115, at *2-3 (S.D. Cal. July 25, 2014); *Jones v. ConAgra Foods, Inc.*, 2014 WL 2702726, at *12-13 (N.D. Cal. June 13, 2014); *Forcellati v. Hyland's, Inc.*, 2014 WL 1410264, at *13 (C.D. Cal. Apr. 9, 2014).

D. The CDA Bars All Non-Misrepresentation Claims Against Apple.

The Communications Decency Act, 47 U.S.C. § 230(c)(1-2), immunizes Apple,[18] as an operator of an "interactive computer service," from liability for content provided by "information content providers," here the App Defendants.[19]

1. The Communications Decency Act: Legal Standards

As this Court has noted, the immunity provided by CDA Section 230(c) is "quite robust." MTD Order at 19. Congress enacted the CDA to "encourage the unfettered and unregulated development of free speech on the Internet, and to promote the development of e-commerce." *Batzel v. Smith*, 333 F.3d 1018, 1027 (9th Cir. 2003). To achieve these goals, Section 230 forbids treating providers of "interactive computer service" as publishers of third-party content and immunizes them from civil claims arising out of the distribution, screening or editing of content created by a third-party. 47 U.S.C. § 230(c). Courts, moreover, must err on the side of finding immunity and should do so at the earliest practical stage. *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254-55 (4th Cir.

[18] This Court found (in the course of dismissing all claims against Apple) that Apple was a "content provider" and not entitled to CDA immunity except as set forth in footnote 12 of the Order. The Court made that ruling, however, with respect to the allegations of *the CAC* and in light of CDA law as it had developed at that time. The SAC contains additional and changed factual allegations, supplementing the pleadings record, and, as set forth above, there have been relevant developments in the fast-changing law concerning the CDA. *See e.g., Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398 (6th Cir. 2014), discussed *infra*. *See generally Bruton v. Gerber Prods. Co.*, 2014 WL 172111, at *7 n.2 (N.D. Cal. Jan. 15, 2014) ("Under Ninth Circuit law, an amended complaint supercedes [*sic*] the original complaint and renders it without legal effect, such that a defendant may challenge an amended complaint in its entirety." (internal citations omitted) (*citing Lacey v. Maricopa Cnty.*, 693 F.3d 896, 927 (9th Cir. 2012)).

[19] Apple does not seek CDA immunity for claims grounded on alleged misrepresentations by Apple. The CDA applies, however, to the SAC's counts for Invasion of Privacy and Conversion and to all of Plaintiffs' remaining claims where the allegations involve any supposed failure by Apple to adequately screen or protect against the access or downloading of address book data, or any other alleged conduct by the App Defendants (aiding and abetting theories) or to any alleged Apple conduct described in footnote 12 of the MTD Order (*e.g.*, providing software development kit, promulgation of review guidelines, enforcement of guidelines).
And, unless based on a duty to correct a material misrepresentation on which Plaintiffs relied, the CDA covers omissions-based claims. It would make no sense for the CDA to immunize Apple for allegedly inadequate screening of unlawful third party content but permit liability for claims that Apple failed to adequately describe the effectiveness (or ineffectiveness) of such screening efforts or capabilities. In analogous decisions, other courts have found that Section 230 shields online distribution platforms from liability for alleged failure to warn or prevent the distribution of tortious or illegal products sold by third-party vendors through their platforms. *See, e.g., Gentry v. eBay*, 99 Cal. App. 4th 816, 821 (2002) (eBay immune from liability for failure to disclose risks associated with sales of fake memorabilia); *Inman v. Technicolor USA, Inc.*, 2011 WL 5829024, at *2 (W.D. Pa. Nov. 18, 2011) (plaintiff could not sue eBay for "fail[ure] to warn of dangers associated" with product sold through eBay's website).

2009) (CDA is "an *immunity from suit* rather than a mere defense to liability")

In carrying out Congressional intent that the CDA confer broad immunity, courts apply an expansive definition of "interactive computer service" and a restrictive definition of "information content provider." MTD Order at 19. The narrow exclusion for "information content providers" is further limited by *Twombly/Iqbal*'s rejection of conclusory allegations and its corresponding requirement of factual allegations setting forth a "plausible" claim versus allegations that are merely "consistent" with liability. *Nemet Chevrolet*, 591 F.3d at 255-56 ("We must determine, in a post-*Iqbal* context, whether the facts pled by [plaintiff] as to the application of CDA immunity, make its claim that [defendant] is an information content provider merely possible or whether Plaintiff has nudged that claim "across the line from conceivable to plausible.") (quoting *Twombly*, 550 U.S. at 570).

In addition to the *Twombly/Iqbal* plausibility requirement, the contention that an "interactive computer service" is also an "information content provider," is subject to two other important limitations. First, courts must precisely determine what portion of the content is illegal. *See, e.g.*, *Gentry*, 99 Cal. App. 4th at 833 n.11 ("[T]he fact appellants allege eBay is an information content provider is irrelevant if eBay did not itself create or develop *the content for which appellants seek to hold it liable* … . The critical issue is whether eBay acted as an information content provider with respect to *the information that appellants claim is false or misleading.*") (emphasis added); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123, 1125 (9th Cir. 2003) ("[A]n 'interactive computer service' qualifies for immunity so long as it does not also function as an 'information content provider' *for the portion of the statement or publication at issue*." The CDA "would still bar … claims unless Matchmaker created or developed *the particular information at issue*.") (emphasis added); *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1168 (9th Cir. 2008) (in order to be deprived of CDA immunity, the interactive computer service must have "contribute[d] materially *to the alleged illegality*"); *see also* MTD Order at 19 quoting *Carafano*.

Second, absent acting as the actual creator of the offending content, unless the service affirmatively *required* the illegal content, it is immune. Here the Ninth Circuit has, again, emphasized that courts are required to err on the side of immunity. In addressing this issue in its *Roommates* opinion, the Ninth Circuit held that the CDA did not protect a housing search website only if it

affirmatively *required* users to answer allegedly unlawful questions about housing preferences. 521 F.3d at 1172 ("Roommate's website is designed to force subscribers to divulge protected characteristics and discriminatory preferences … ."). Answering the dissenters' concerns that the majority opinion undermined the CDA's broad immunity coverage, the *Roommates* majority emphasized that its opinion was narrowly confined to situations where the defendant *required* users to provide the exact content that created the cause of action:

> Here, the part of the profile that is alleged to offend the Fair Housing Act and state housing discrimination laws …… is provided by subscribers in response to Roommate's questions, which they cannot refuse to answer if they want to use defendant's services. *By requiring subscribers to provide the information as a condition of accessing its service*, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information.

Id. at 1165-66 (emphasis added).

To drive home the narrow scope of the exception, the *Roommates* Court cautioned against allowing plaintiffs to evade CDA immunity through a less demanding standard:

> We must keep firmly in mind that this is an immunity statute we are expounding … . Websites are complicated enterprises, and *there will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity*, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites, *fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties.*

Id. at 1174 (emphasis added).

The standard enunciated by the Ninth Circuit is thus clear: An interactive computer service will be liable as an "information content provider" if, and only if, it created or required the illegal content; "promotion" or "encouragement" will not suffice. Other Circuits are in accord. Subsequent to this Court's MTD Order, the Sixth Circuit overturned a district court denial of CDA immunity that had mischaracterized *Roommates* as a more lax "encouragement" standard. *Dirty World Entm't Recordings LLC*, 755 F.3d at 414-15. In elucidating the line between developing or acquiring actionable content and merely encouraging or providing a forum for it, the Sixth Circuit relied on the Ninth Circuit's *Roommates* decision, explaining:

> We do not adopt the district court's encouragement test of immunity under the CDA. The district court misapprehended how other circuits, particularly the Ninth Circuit in *Roommates*, have separated what constitutes "development" in § 230(f)(3) from what does not. The district court elided the crucial distinction between, on the one hand, taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable … . In

> *Roommates*, the website was responsible for the alleged discrimination by requiring users to submit protected characteristics and hiding listings based on those submissions.

Id. at 414.

As set forth below, controlling law and the record pleadings, as now supplemented by the SAC allegations, compel the conclusion that, aside from affirmative misrepresentation claims, the CDA immunizes Apple's alleged conduct here.

2. The App Store is an "interactive computer service."

There can be no serious dispute that Apple's App Store is an "interactive computer service." The CDA defines "interactive computer service" expansively to include "*any* information service, system, or access software provider that provides or enables computer access by multiple users to a computer server …" 47 U.S.C. § 230(f)(2). The statute defines an "access software provider" as one that provides enabling tools to filter, screen, pick, choose, analyze, digest, search, forward, organize, and reorganize content. 47 U.S.C. § 230(f)(4)(A)-(C). Plaintiffs have alleged, among other things, that users of iOS products can "wirelessly browse for and obtain … apps" from the App Store; that the App Store is a "centralized repository of apps available for iDevices"; and that "[a]ll iDevices are tethered and networked to the App Store through their on-device App Store app." CAC ¶¶173-74.[20] These allegations show that the App Store is a networked software applications provider, hosted on a server, that App Store users employ to screen and choose among applications. Other courts have treated similar on-line stores for downloading applications as interactive computer services within the CDA's definition. *See, e.g.*, *Evans v. Hewlett-Packard Co.*, 2013 WL 5594717 (N.D. Cal. Oct. 10, 2013).

3. Apple is not an "information content provider" regarding the "content at issue."

Plaintiffs cannot point to any Apple statement that condoned, let alone required, collecting address book data without permission. To the contrary, the Plaintiffs have repeatedly alleged that Apple prohibited that conduct, and that the App Developers were subject to those prohibitions:

- The App Store Review Guidelines set forth the technical, design, and content guidelines Apple will use when reviewing an App for inclusion in Apple's App Store. These guidelines state that Apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." SAC

[20] In re-pleading the SAC, Plaintiffs removed almost all of their previous allegations regarding how the App Store operates, including the above-quoted allegations. That does not prevent the Court from considering those allegations and, in fact, their deletion in the SAC serves only to highlight the implausibility of inconsistent allegations and arguments. *See supra* at III.3.C.

¶47.

- "Any form of user or device data collection … must comply with all applicable privacy laws and regulations as well as any Apple program requirements related to such aspects, including but not limited to any notice or consent requirements." SAC Ex. J.
- "Apple continuously used this phrase and/or variations of it in all subsequent iterations of its Developer Program License Agreement." SAC ¶76xi.
- "Apple and the App Defendants are subject to standards and duties of care established by Apple … . Affirmative duties include … building, offering, selling, or deploying apps that do not … take or use iDevice owners' property (iDevices or mobile address books), expose iDevice owners' private information (mobile address books or their contents), or enable others to do so." CAC ¶198 (emphasis added).
- Apple's App Store Review Guidelines mandate that: (i) private data not be obtained from an iDevice without owner consent; (ii) apps not have secret hidden features; and (iii) apps comply with local legal requirements in all jurisdictions in which the app is available (subjecting each to the highest applicable legal standard). CAC ¶204.
- The App Defendants must abide by standards specified in Apple's Program terms, standards, documentation, guides, guidelines (including Apple's App Store Review Guidelines) and agreements (including Apple's IDPLA and SDK agreements)." CAC ¶201.21

Further, according to Plaintiffs, Apple not only prohibited (with words) the alleged unlawful content at issue, it implemented technical measures to prevent app developers from disregarding those prohibitions. Plaintiffs' allegations describe how app developers overrode or broke technical safeguards Apple had in place to prevent the alleged conduct at issue:

- "Instagram's conduct in overriding Apple's purported protections of users' privacy and security devalued the iDevice for its users. Users [did not know] that the Instagram App would circumvent both internal and external safeguards designed for the protection of their private and personal information residing on the iDevice." CAC ¶335; *see also id.* ¶343.
- "Each App Defendants has violated California Penal Code § 502(c)(1) by … deceiv[ing] Plaintiffs and Class Members into accepting, downloading, and using the App(s) that contained undisclosed code that would circumvent protections on the iDevices that were designed to keep information therein safe, secure, and private." *Id.* ¶554.

All of these allegations contradict the proposition that Apple developed, created, or required apps that would collect user address book information without permission. Accordingly, to find that Apple is a "content provider" and deprived of CDA immunity, in the face of Plaintiffs' own allegations, would be directly contrary to the stated basis for the majority opinion in the Ninth Circuit's *Roommates* decision.

[21] Additional Plaintiff allegations of Apple's prohibition of the alleged conduct at issue and/or Apple's enforcement of those prohibitions include CAC ¶¶114 ("copying address book data … without a user's consent is against Apple's rules"); 137 ("Apps that collect or transmit a user's contact data without their prior permission are in violation of [Apple's] guidelines"); 140 ("As exemplified by Apple's 2008 delisting of the Aurora Feint App, the 2009 delisting of the Google Voice App, and Apple's statements in its FCC Letter, Apple deems apps that relay iDevice owners' mobile address book to developers' (or third-party) servers without the iDevice owner's prior approval to be inappropriate for the App Store and for consumer iDevices"); *see also* SAC ¶¶83, 84, 87; CAC ¶¶144, 194, 204, 205, 219, 223, 287, 288.

In the face of these factual allegations precluding the conclusion that Apple is a content provider of the content at issue, the SAC, like its predecessor, relies almost exclusively,[22] on a single statement from Apple's Human Interface Guidelines ("HIG"), for the conclusory allegation that Apple developer materials "teach App developers … how to code and build Apps that non-consensually access, use and upload the mobile address books maintained on Apple iDevices … ." SAC at ¶52. But the HIG cannot reasonably be construed in such a manner. All the HIG says on the issue is:

> "Get information from iOS, *when appropriate*. People store lots of information on their devices. *When it makes sense*, don't force people to give you information you can easily find for yourself, such as their contacts or calendar information." SAC at ¶88 (emphasis added).

Nothing in that statement supports the notion that Apple encouraged, let alone required, app developers to take or upload data "non-consensually."

Moreover, Plaintiffs take their quotes from the HIG out of their larger context. It is plain from the face of the HIG that it is not a "requirements" or a "prohibitions" document. Rather, it is a general guidebook on how to build aesthetically pleasing, user-friendly apps. It describes itself, and its fundamental purpose, as follows:

- "iOS Human Interface Guidelines describes the guidelines and principles that help you design a superlative user interface and user experience for your iOS app."
- "It's essential to keep the user experience uppermost in your mind as you design every aspect of your app, from the way you enable a task, to the way your app starts and stops, to the way you use a button. Discover the guidelines that influence the look and behavior of your app, in matters both general and specific."

RJN Ex. H, at 8, 9. And, as Apple's instructions to developers make plain, the HIG is a *companion document* to Apple's Review Guidelines, and the two must be applied in tandem: "Before you submit your app for approval, ensure that it follows the technical, design, and content specifications detailed in the App Store Review Guidelines and Human Interface Guidelines." RJN Ex.I, at 2. And, as noted above, Plaintiffs repeatedly acknowledge that the App Review Guidelines prohibit taking data without permission. Therefore, when read in context and in combination, the HIG provides the general advice that apps should access data on the device "when appropriate" instead of requiring users to enter it

[22] The SAC also vaguely accuses Apple "developer websites" and "tutorials" of teaching app developers to build the offending features of their apps, yet there is not a single line identifying any of those developer sites or tutorials or their content. And, while the SAC alleges that the HIG advised app developers to delay presenting users with any function requiring a login until the user first had a chance to navigate the app to try it out, SAC ¶88, Plaintiffs never explain how a user login has anything to do with app security, let alone with non-consensual data transfers.

themselves, and the App Review Guidelines explain unambiguously the "when appropriate" limitations on the HIG advice, *i.e*, not without permission.

There is nothing in the SAC that identifies how any Apple software tools or guidelines encouraged or facilitated, let alone required, any App Defendant to collect Plaintiffs' data *without permission*. To deprive Apple of the protections of the CDA, based on general advice in the HIG concerning how to enhance user experience—which has nothing to do with non-consensual data transfers—reads something into that document that simply is not there. Doing so would contravene controlling law set forth in the Ninth Circuit's *Roommates* decision.

Finally, declining CDA immunity here on the basis of Plaintiffs' conclusory allegations would violate *Twombly/Iqbal* pleading principles. The plausibility of Plaintiffs' claims that Apple created offending content should be assessed in the light that Plaintiffs have never offered any explanation of the possible motive Apple could have had for participating in this purported scheme to violate its own rules. *See Chang v. Rockridge Manor Condominium*, 2008 WL 413741, at *10 (N.D. Cal. Feb. 13, 2008) ("Plaintiffs have failed to articulate even a conceivable basis for conspiracy, let alone a plausible one."); *Delalla v. Hanover Ins.*, 2010 WL 3259816, at *10 (E.D. Pa. Aug. 17, 2010), *aff'd* 660 F.3d 180 (3d Cir. 2011) ("Complaint did not plead enough facts to demonstrate plausibly why Hanover and … Defendants, as alleged, would have a motive or reason to conspire together.") For example, they do not allege that Apple derives a financial or other benefit from apps that access confidential information without user consent. In fact, Plaintiffs' theory that Apple uses its dedication to data security as a market-differentiator makes it highly implausible that Apple would intentionally allow apps to flout its data security rules.

IV. CONCLUSION

For the foregoing reasons, the SAC's claims against Apple should be dismissed with prejudice.

Dated: August 22, 2014

HOGAN LOVELLS US LLP

By: */s/ Robert B. Hawk*
Robert B. Hawk

Attorneys for Defendant
APPLE INC.